

Hacking Articles

Raj Chandel's Blog



Menu

[Home](#) » [Penetration Testing](#) » [Comprehensive Guide on Gobuster Tool](#)

Penetration Testing

Comprehensive Guide on Gobuster Tool

October 19, 2018 By Raj Chandel

Hello Friend!! Today we are going demonstrate URLs and DNS brute force attack for extracting Directories and files from inside URLs and sub-domains from DNS by using “Gobuster-tool”.

Table of Content

- Introduction & Installation
- Using Wordlist for Directory Brute-Force
- Obtaining Full Path for a directory or file
- Hide Status Code
- Verbose Mode
- Identify Content-Length
- Disable Banner
- User-Agent Mode
- Obtain Result with Specify Status Code
- Timeout
- Appending Forward slash
- Saving Output Result inside Text File
- Enumerating Directory with Specific Extension List
- Follow Redirect

- HTTP AUTHORIZATION (-u username: password)
- DNS Mode
- Set Threads Number
- Obtain Sub domain IPs
- Force Processing Brute Force
- Hide Process of Extracting
- Extracting CNAME Records

Introduction & Installation

Gobuster is a tool used to brute-force on URLs (directories and files) in websites and DNS subdomains. Gobuster can be downloaded through the apt- repository and thus execute the following command for installing it.

```
apt-get install gobuster
```

A terminal window on a Kali Linux system showing the command 'apt-get install gobuster' being executed. The output shows that several packages were automatically installed and are no longer needed, and that the new package 'gobuster' will be installed. The terminal text is as follows:

```
root@kali:~# apt-get install gobuster ↩
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer
  gir1.2-mutter-2 gvfs-bin libann0 libavahi-gobject0 libcamel-1.2-61
  libqgis-networkanalysis2.18.23 libqgis-server2.18.23 libqgispython2
Use 'apt autoremove' to remove them.
The following NEW packages will be installed:
  gobuster
0 upgraded, 1 newly installed, 0 to remove and 11 not upgraded.
Need to get 1,281 kB of archives.
After this operation, 4,297 kB of additional disk space will be used.
Get:1 http://mirrors.neusoft.edu.cn/kali kali-rolling/main amd64 gobus
Fetched 1,281 kB in 4s (307 kB/s)
Selecting previously unselected package gobuster.
(Reading database ... 352070 files and directories currently installed
Preparing to unpack .../gobuster_2.0.0-0kali1_amd64.deb ...
Unpacking gobuster (2.0.0-0kali1) ...
Setting up gobuster (2.0.0-0kali1) ...
```

When it will get installed, you can interact with it and can perceive all available option with the help of the following command.

```
gobuster -h
```

Common Parameters

- -fw – force processing of a domain with wildcard results.
- -np – hide the progress output.
- -m <mode> – which mode to use, either dir or dns (default: dir).
- -q – disables banner/underline output.
- -t <threads> – number of threads to run (default: 10).
- -u <url/domain> – full URL (including scheme), or base domain name.
- -v – verbose output (show all results).
- -w <wordlist> – path to the wordlist used for brute forcing (use – for stdin).

Dir mode Parameter

- -a <user agent string> – specify a user agent string to send in the request header.
- -c – use this to specify any cookies that you might need (simulating auth).
- -e – specify the extended mode that renders the full URL.
- -f – append / for directory brute forces.
- -k – Skip verification of SSL certificates.
- -l – show the length of the response.
- -n – “no status” mode, disables the output of the result’s status code.
- -o <file> – specify a file name to write the output to.
- -p <proxy url> – specify a proxy to use for all requests (scheme much match the URL scheme).
- -r – follow redirects.
- -s <status codes> – comma-separated set of the list of status codes to be deemed a “positive” (default: 200,204,301,302,307).
- -x <extensions> – list of extensions to check for, if any.
- -P – HTTP Authorization password (Basic Auth only, prompted if missing).
- -U – HTTP Authorization username (Basic Auth only).
- -to – HTTP timeout. Examples: 10s, 100ms, 1m (default: 10s).

DNS mode Parameters

- -cn – show CNAME records (cannot be used with ‘-i’ option).
- -i – show all IP addresses for the result.

```
root@kali:~# gobuster -h ↩
Usage of gobuster:
  -P string
      Password for Basic Auth (dir mode only)
  -U string
      Username for Basic Auth (dir mode only)
  -a string
      Set the User-Agent string (dir mode only)
  -c string
      Cookies to use for the requests (dir mode only)
  -cn
      Show CNAME records (dns mode only, cannot be used with '-i' option)
  -e
      Expanded mode, print full URLs
  -f
      Append a forward-slash to each directory request (dir mode only)
  -fw
      Force continued operation when wildcard found
  -i
      Show IP addresses (dns mode only)
  -k
      Skip SSL certificate verification
  -l
      Include the length of the body in the output (dir mode only)
  -m string
      Directory/File mode (dir) or DNS mode (dns) (default "dir")
  -n
      Don't print status codes
  -np
      Don't display progress
  -o string
      Output file to write results to (defaults to stdout)
  -p string
      Proxy to use for requests [http(s)://host:port] (dir mode only)
  -q
      Don't print the banner and other noise
  -r
      Follow redirects
  -s string
      Positive status codes (dir mode only) (default "200,204,301,302,307,403")
  -t int
      Number of concurrent threads (default 10)
  -to duration
      HTTP Timeout in seconds (dir mode only) (default 10s)
  -u string
      The target URL or Domain
  -v
      Verbose output (errors)
  -w string
      Path to the wordlist
  -x string
      File extension(s) to search for (dir mode only)
```

Using Wordlist for Directory Brute-Force

You can use **-w option** for using a particular wordlist, for example, common.txt or medium.txt to launch a brute-force attack for extracting web directories or files from inside the target URL.

```
gobuster -u http://192.168.1.108/dvwa -w /usr/share/wordlists/dirb/common.txt
```

The above command will dump the all possible files and directories with the help of common.txt wordlist.

```
root@kali:~# gobuster -u http://192.168.1.108/dvwa -w /usr/share/wordlists/dirb/common.txt

=====
Gobuster v2.0.0                  OJ Reeves (@TheColonial)
=====
[+] Mode : dir
[+] Url/Domain : http://192.168.1.108/dvwa/
[+] Threads : 10
[+] Wordlist : /usr/share/wordlists/dirb/common.txt
[+] Status codes : 200,204,301,302,307,403
[+] Timeout : 10s
=====
2018/10/17 13:21:03 Starting gobuster
=====
/.hta (Status: 403)
/.htpasswd (Status: 403)
/.htaccess (Status: 403)
/about (Status: 302)
/config (Status: 301)
/docs (Status: 301)
/external (Status: 301)
/favicon.ico (Status: 200)
/index (Status: 302)
/index.php (Status: 302)
/instructions (Status: 302)
/logout (Status: 302)
/login (Status: 200)
/php.ini (Status: 200)
/phpinfo.php (Status: 302)
/phpinfo (Status: 302)
/README (Status: 200)
/robots (Status: 200)
/robots.txt (Status: 200)
/security (Status: 302)
/setup (Status: 200)
=====
2018/10/17 13:21:05 Finished
=====
```

Obtaining Full Path for a directory or file

Using **-e option** provides a more significant result, as it Prints complete URL when extracting any file or directories.

```
gobuster -e -u http://192.168.1.108/dvwa -w /usr/share/wordlists/dirb/common.t
```

You can compare the following output result from the previous result.

```
root@kali:~# gobuster -e -u http://192.168.1.108/dvwa -w /usr/share/wordlists/dirb/common.txt

=====
Gobuster v2.0.0                OJ Reeves (@TheColonial)
=====
[+] Mode           : dir
[+] Url/Domain     : http://192.168.1.108/dvwa/
[+] Threads       : 10
[+] Wordlist        : /usr/share/wordlists/dirb/common.txt
[+] Status codes   : 200,204,301,302,307,403
[+] Expanded       : true
[+] Timeout        : 10s
=====
2018/10/17 13:21:35 Starting gobuster
=====
http://192.168.1.108/dvwa/.htaccess (Status: 403)
http://192.168.1.108/dvwa/.htpasswd (Status: 403)
http://192.168.1.108/dvwa/.hta (Status: 403)
http://192.168.1.108/dvwa/about (Status: 302)
http://192.168.1.108/dvwa/config (Status: 301)
http://192.168.1.108/dvwa/docs (Status: 301)
http://192.168.1.108/dvwa/external (Status: 301)
http://192.168.1.108/dvwa/favicon.ico (Status: 200)
http://192.168.1.108/dvwa/index (Status: 302)
http://192.168.1.108/dvwa/index.php (Status: 302)
http://192.168.1.108/dvwa/instructions (Status: 302)
http://192.168.1.108/dvwa/logout (Status: 302)
http://192.168.1.108/dvwa/login (Status: 200)
http://192.168.1.108/dvwa/php.ini (Status: 200)
http://192.168.1.108/dvwa/phpinfo (Status: 302)
http://192.168.1.108/dvwa/phpinfo.php (Status: 302)
http://192.168.1.108/dvwa/README (Status: 200)
http://192.168.1.108/dvwa/robots.txt (Status: 200)
http://192.168.1.108/dvwa/robots (Status: 200)
http://192.168.1.108/dvwa/security (Status: 302)
http://192.168.1.108/dvwa/setup (Status: 200)
=====
2018/10/17 13:21:36 Finished
=====
root@kali:~#
```

Hide Status Code

Using **-n Option** “no status” mode, it prints the output of the results without displaying the status code.

```
gobuster -u http://192.168.1.108/dvwa -w /usr/share/wordlists/dirb/common.txt
```

The above command will dump all possible files and directory without displaying their status code.

```
root@kali:~# gobuster -u http://192.168.1.108/dvwa -w /usr/share/wordlists/dirb/common.txt -n

=====
Gobuster v2.0.0                OJ Reeves (@TheColonial)
=====
[+] Mode           : dir
[+] Url/Domain     : http://192.168.1.108/dvwa/
[+] Threads       : 10
[+] Wordlist       : /usr/share/wordlists/dirb/common.txt
[+] Status codes   : 200,204,301,302,307,403
[+] No status     : true
[+] Timeout       : 10s
=====

2018/10/17 13:22:10 Starting gobuster
=====
/.hta
/.htaccess
/.htpasswd
/about
/config
/docs
/external
/favicon.ico
/index.php
/index
/instructions
/login
/logout
/php.ini
/phpinfo.php
/phpinfo
/README
/robots
/robots.txt
/security
/setup
=====

2018/10/17 13:22:11 Finished
=====
```

Verbose Mode

Using **-v option** – it enables the verbose parameter and makes brute-force attack vigorously on each file or directory.

```
gobuster -u http://192.168.1.108/dvwa -w /usr/share/wordlists/dirb/common.txt
```

As you can observe from the following option that, this time it has to dump the result including status 404 for missing directories or files.

```
root@kali:~# gobuster -u http://192.168.1.108/dvwa -w /usr/share/wordlists/dirb/common.txt -v
=====
Gobuster v2.0.0                OJ Reeves (@TheColonial)
=====
[+] Mode           : dir
[+] Url/Domain     : http://192.168.1.108/dvwa/
[+] Threads       : 10
[+] Wordlist       : /usr/share/wordlists/dirb/common.txt
[+] Status codes   : 200,204,301,302,307,403
[+] Verbose       : true
[+] Timeout       : 10s
=====
2018/10/17 13:22:41 Starting gobuster
=====
Missed: /.bashrc (Status: 404)
Missed: /.cvsignore (Status: 404)
Missed: /.cvs (Status: 404)
Missed: /.cache (Status: 404)
Found: /.hta (Status: 403)
Missed: /.history (Status: 404)
Found: /.htaccess (Status: 403)
Missed: /.git/HEAD (Status: 404)
Missed: /.passwd (Status: 404)
Missed: /.forward (Status: 404)
Missed: /.config (Status: 404)
Missed: /.perf (Status: 404)
Missed: /.listing (Status: 404)
Missed: /.listings (Status: 404)
Missed: /.mysql_history (Status: 404)
Missed: /.profile (Status: 404)
Missed: /.subversion (Status: 404)
Missed: /.web (Status: 404)
Missed: /.svn (Status: 404)
Missed: /.rhosts (Status: 404)
Missed: /.svn/entries (Status: 404)
Missed: /.sh_history (Status: 404)
Missed: /.swf (Status: 404)
Missed: /_ (Status: 404)
```

Identify Content-Length

Using **-l option** enables content-length parameter which displays the size of the response.

A Content-Length header is a number denoting and the exact byte length of the HTTP body for extracted file or directory.

```
gobuster -u http://192.168.1.108/dvwa -w /usr/share/wordlists/dirb/common.txt
```



```
root@kali:~# gobuster -u http://192.168.1.108/dvwa -w /usr/share/wordlists/dirb/common.txt -l
=====
Gobuster v2.0.0                OJ Reeves (@TheColonial)
=====
[+] Mode           : dir
[+] Url/Domain     : http://192.168.1.108/dvwa/
[+] Threads       : 10
[+] Wordlist       : /usr/share/wordlists/dirb/common.txt
[+] Status codes   : 200,204,301,302,307,403
[+] Show length    : true
[+] Timeout       : 10s
=====
2018/10/17 13:23:15 Starting gobuster
=====
/.htaccess (Status: 403) [Size: 300]
/.hta (Status: 403) [Size: 295]
/.htpasswd (Status: 403) [Size: 300]
/about (Status: 302) [Size: 0]
/config (Status: 301) [Size: 325]
/docs (Status: 301) [Size: 323]
/external (Status: 301) [Size: 327]
/favicon.ico (Status: 200) [Size: 1406]
/index.php (Status: 302) [Size: 0]
/index (Status: 302) [Size: 0]
/instructions (Status: 302) [Size: 0]
/login (Status: 200) [Size: 1289]
/logout (Status: 302) [Size: 0]
/php.ini (Status: 200) [Size: 148]
/phpinfo.php (Status: 302) [Size: 0]
/phpinfo (Status: 302) [Size: 0]
/README (Status: 200) [Size: 4934]
/robots (Status: 200) [Size: 26]
/robots.txt (Status: 200) [Size: 26]
/security (Status: 302) [Size: 0]
/setup (Status: 200) [Size: 3549]
=====
2018/10/17 13:23:16 Finished
=====
```

Disable Banner

Gobuster always adds the banner to specify the brief introduction of applied options while launching a brute force attack. By using **-q option** we can disable the banner to hide additional information.

```
gobuster -u http://192.168.1.108/dvwa -w /usr/share/wordlists/dirb/common.txt
```

From the given below image, you can perceive the difference between the last output results and in the current result.

```
root@kali:~# gobuster -u http://192.168.1.108/dvwa -w /usr/share/wordlists/dirb/common.txt -q
/.htaccess (Status: 403)
/.htpasswd (Status: 403)
/.hta (Status: 403)
/about (Status: 302)
/config (Status: 301)
/docs (Status: 301)
/external (Status: 301)
/favicon.ico (Status: 200)
/index.php (Status: 302)
/index (Status: 302)
/instructions (Status: 302)
/login (Status: 200)
/logout (Status: 302)
/php.ini (Status: 200)
/phpinfo (Status: 302)
/phpinfo.php (Status: 302)
/README (Status: 200)
/robots.txt (Status: 200)
/robots (Status: 200)
/security (Status: 302)
/setup (Status: 200)
```



User-Agent Mode

Using **-an option** enables User-Agent mode to specify a user agent string to send in the request header for extracting directories and files from inside the target URL.

```
gobuster -u http://192.168.1.108/dvwa -w /usr/share/wordlists/dirb/common.txt
```

```

root@kali:~# gobuster -u http://192.168.1.108/dvwa -w /usr/share/wordlists/dirb/common.txt -a Mozilla/5.0 -fw
=====
Gobuster v2.0.0                OJ Reeves (@TheColonial)
=====
[+] Mode       : dir
[+] Url/Domain  : http://192.168.1.108/dvwa/
[+] Threads    : 10
[+] Wordlist    : /usr/share/wordlists/dirb/common.txt
[+] Status codes : 200,204,301,302,307,403
[+] User Agent  : Mozilla/5.0
[+] Timeout    : 10s
=====
2018/10/17 13:24:50 Starting gobuster
=====
/.hta (Status: 403)
/.htpasswd (Status: 403)
/.htaccess (Status: 403)
/about (Status: 302)
/config (Status: 301)
/docs (Status: 301)
/external (Status: 301)
/favicon.ico (Status: 200)
/index.php (Status: 302)
/index (Status: 302)
/instructions (Status: 302)
/logout (Status: 302)
/login (Status: 200)
/php.ini (Status: 200)
/phpinfo.php (Status: 302)
/phpinfo (Status: 302)
/README (Status: 200)
/robots (Status: 200)
/robots.txt (Status: 200)
/security (Status: 302)
/setup (Status: 200)
=====

```

Obtain Result with Specify Status Code

Using **-s Option** enables the status code for specific value such as 302, 200, 403, and 404 and so on to obtain certain request pages.

```

gobuster -u http://192.168.1.108/dvwa -w /usr/share/wordlists/dirb/common.txt
gobuster -u http://192.168.1.108/dvwa -w /usr/share/wordlists/dirb/common.txt

```

From the given below image, you can take reference for the output result obtained for the above commands.

```
root@kali:~# gobuster -u http://192.168.1.108/dvwa -w /usr/share/wordlists/dirb/common.txt -s 302
=====
Gobuster v2.0.0                OJ Reeves (@TheColonial)
=====
[+] Mode          : dir
[+] Url/Domain    : http://192.168.1.108/dvwa/
[+] Threads      : 10
[+] Wordlist      : /usr/share/wordlists/dirb/common.txt
[+] Status codes : 302
[+] Timeout      : 10s
=====
2018/10/17 13:25:14 Starting gobuster
=====
/about (Status: 302)
/index.php (Status: 302)
/index (Status: 302)
/instructions (Status: 302)
/logout (Status: 302)
/phpinfo (Status: 302)
/phpinfo.php (Status: 302)
/security (Status: 302)
=====
2018/10/17 13:25:15 Finished
=====
root@kali:~# gobuster -u http://192.168.1.108/dvwa -w /usr/share/wordlists/dirb/common.txt -s 200
=====
Gobuster v2.0.0                OJ Reeves (@TheColonial)
=====
[+] Mode          : dir
[+] Url/Domain    : http://192.168.1.108/dvwa/
[+] Threads      : 10
[+] Wordlist      : /usr/share/wordlists/dirb/common.txt
[+] Status codes : 200
[+] Timeout      : 10s
=====
2018/10/17 13:25:20 Starting gobuster
=====
/favicon.ico (Status: 200)
/login (Status: 200)
/php.ini (Status: 200)
/README (Status: 200)
/robots (Status: 200)
/robots.txt (Status: 200)
/setup (Status: 200)
=====
2018/10/17 13:25:21 Finished
=====
```

Timeout

Using **-to option** enables the timeout parameter for HTTP request and 10 second is the Default time limit for the HTTP request.

```
gobuster -u http://192.168.1.108/dvwa -w /usr/share/wordlists/dirb/common.txt
```

```
root@kali:~# gobuster -u http://192.168.1.108/dvwa -w /usr/share/wordlists/dirb/common.txt -to 10s

=====
Gobuster v2.0.0                                OJ Reeves (@TheColonial)
=====
[+] Mode           : dir
[+] Url/Domain     : http://192.168.1.108/dvwa/
[+] Threads       : 10
[+] Wordlist       : /usr/share/wordlists/dirb/common.txt
[+] Status codes  : 200,204,301,302,307,403
[+] Timeout       : 10s
=====
2018/10/17 13:25:50 Starting gobuster
=====
```

Appending Forward slash

Using **-f option**, appending the forward slash while making brute-force attack on the target URL.

```
gobuster -u http://192.168.1.108/dvwa -w /usr/share/wordlists/dirb/common.txt
```

```
root@kali:~# gobuster -u http://192.168.1.108/dvwa -w /usr/share/wordlists/dirb/common.txt -f

=====
Gobuster v2.0.0                                OJ Reeves (@TheColonial)
=====
[+] Mode           : dir
[+] Url/Domain     : http://192.168.1.108/dvwa/
[+] Threads       : 10
[+] Wordlist       : /usr/share/wordlists/dirb/common.txt
[+] Status codes  : 200,204,301,302,307,403
[+] Add Slash     : true
[+] Timeout       : 10s
=====
2018/10/17 13:26:15 Starting gobuster
=====
/.hta/ (Status: 403)
/.htpasswd/ (Status: 403)
/.htaccess/ (Status: 403)
/about/ (Status: 302)
/config/ (Status: 200)
/docs/ (Status: 200)
/external/ (Status: 200)
/index.php/ (Status: 302)
/index/ (Status: 302)
/instructions/ (Status: 302)
/logout/ (Status: 302)
/login/ (Status: 200)
/phpinfo.php/ (Status: 302)
/phpinfo/ (Status: 302)
/security/ (Status: 302)
/setup/ (Status: 200)
```

Saving Output Result inside Text File

Using **-o option** enables saving output result parameter in a text file which can be useful in the future.

```
gobuster -u http://192.168.1.108/dvwa -w /usr/share/wordlists/dirb/common.txt
```

We can ensure the result.txt file with the help of cat command

```
cat result.txt
```

```
root@kali:~# gobuster -u http://192.168.1.108/dvwa -w /usr/share/wordlists/dirb/common.txt -o result.txt
=====
Gobuster v2.0.0 www.hackingarticles.in OJ Reeves (@TheColonial)
=====
[+] Mode           : dir
[+] Url/Domain     : http://192.168.1.108/dvwa/
[+] Threads       : 10
[+] Wordlist        : /usr/share/wordlists/dirb/common.txt
[+] Status codes   : 200,204,301,302,307,403
[+] Timeout        : 10s
=====
2018/10/17 13:26:53 Starting gobuster
=====
/.htaccess (Status: 403)
/.hta (Status: 403)
/.htpasswd (Status: 403)
/about (Status: 302)
/config (Status: 301)
/docs (Status: 301)
/external (Status: 301)
/favicon.ico (Status: 200)
/index.php (Status: 302)
/index (Status: 302)
/instructions (Status: 302)
/login (Status: 200)
/logout (Status: 302)
/php.ini (Status: 200)
/phpinfo (Status: 302)
/phpinfo.php (Status: 302)
/README (Status: 200)
/robots.txt (Status: 200)
/robots (Status: 200)
/security (Status: 302)
/setup (Status: 200)
=====
2018/10/17 13:26:54 Finished
=====
root@kali:~# cat result.txt
/.htaccess (Status: 403)
/.hta (Status: 403)
/.htpasswd (Status: 403)
/about (Status: 302)
/config (Status: 301)
/docs (Status: 301)
/external (Status: 301)
```

Enumerating Directory with Specific Extension List

There are a lot of situations where we need to extract the directories of a specific extension over the target server, and then we can use the **-X parameter** of this scan. This parameter accepts the file extension name and then searches the given extension files over the target server or machine.

```
gobuster -u http://192.168.1.108/dvwa -w /usr/share/wordlists/dirb/common.txt
```

```
root@kali:~# gobuster -u http://192.168.1.108/dvwa -w /usr/share/wordlists/dirb/common.txt -x .php

=====
Gobuster v2.0.0                OJ Reeves (@TheColonial)
=====
[+] Mode           : dir
[+] Url/Domain     : http://192.168.1.108/dvwa/
[+] Threads       : 10
[+] Wordlist       : /usr/share/wordlists/dirb/common.txt
[+] Status codes  : 200,204,301,302,307,403
[+] Extensions   : php
[+] Timeout       : 10s
=====

2018/10/17 13:31:29 Starting gobuster
=====
/.hta (Status: 403)
/.hta.php (Status: 403)
/.htpasswd (Status: 403)
/.htpasswd.php (Status: 403)
/.htaccess (Status: 403)
/.htaccess.php (Status: 403)
/about (Status: 302)
/about.php (Status: 302)
/config (Status: 301)
/docs (Status: 301)
/external (Status: 301)
/favicon.ico (Status: 200)
/index.php (Status: 302)
/index (Status: 302)
/index.php (Status: 302)
/instructions (Status: 302)
/instructions.php (Status: 302)
/logout (Status: 302)
/logout.php (Status: 302)
/login (Status: 200)
/login.php (Status: 200)
/php.ini (Status: 200)
/phpinfo.php (Status: 302)
/phpinfo (Status: 302)
/phpinfo.php (Status: 302)
/README (Status: 200)
/robots (Status: 200)
/robots.txt (Status: 200)
/security (Status: 302)
```

Follow Redirect

Using **-r options** enables redirect parameter which redirects HTTP request to another and modifies the Status code for a directory or file.

```
gobuster -u http://192.168.1.108/dvwa -w /usr/share/wordlists/dirb/common.txt
gobuster -u http://192.168.1.108/dvwa -r -w /usr/share/wordlists/dirb/common.t
```

You can compare the output result of the default scan with redirect output result.

```
root@kali:~# gobuster -u http://192.168.1.108/dvwa -w /usr/share/wordlists/dirb/common.txt -q
/.hta (Status: 403)
/.htaccess (Status: 403)
/.htpasswd (Status: 403)
/about (Status: 302)
/config (Status: 301)
/docs (Status: 301)
/external (Status: 301)
/favicon.ico (Status: 200)
/index.php (Status: 302)
/index (Status: 302)
/instructions (Status: 302)
/login (Status: 200)
/logout (Status: 302)
/php.ini (Status: 200)
/phpinfo.php (Status: 302)
/phpinfo (Status: 302)
/README (Status: 200)
/robots.txt (Status: 200)
/robots (Status: 200)
/security (Status: 302)
/setup (Status: 200)
root@kali:~# gobuster -u http://192.168.1.108/dvwa -r -w /usr/share/wordlists/dirb/common.txt -q
/.hta (Status: 403)
/.htaccess (Status: 403)
/.htpasswd (Status: 403)
/about (Status: 200)
/config (Status: 200)
/docs (Status: 200)
/external (Status: 200)
/favicon.ico (Status: 200)
/index.php (Status: 200)
/index (Status: 200)
/instructions (Status: 200)
/login (Status: 200)
/logout (Status: 200)
/php.ini (Status: 200)
/phpinfo (Status: 200)
/phpinfo.php (Status: 200)
/README (Status: 200)
/robots.txt (Status: 200)
/robots (Status: 200)
/security (Status: 200)
```

HTTP AUTHORIZATION (-u username: password)

HTTP Authentication/Authentication mechanisms are all based on the use of 401-status code and WWW-Authenticate response header. The most widely used HTTP

authentication mechanisms are **Basic**. The client sends the user name and password as un-encrypted base64 encoded text.

So, in order to bypass this kind of authentication with the help of Gobuster we have used the command below:

```
gobuster -u http://testphp.vulnweb.com/login.php -w /usr/share/wordlists/dirb/
```

As a result, it is shown Status -code 200 for the test: test and authorized credential on target URL.

```
root@kali:~# gobuster -u http://testphp.vulnweb.com/login.php -w /usr/share/wordlists/dirb/common.txt -U test -P test
=====
Gobuster v2.0.0                                OJ Reeves (@TheColonial)
=====
[+] Mode           : dir
[+] Url/Domain     : http://testphp.vulnweb.com/login.php/
[+] Threads       : 10
[+] Wordlist       : /usr/share/wordlists/dirb/common.txt
[+] Status codes  : 200,204,301,302,307,403
[+] Auth User     : test
[+] Timeout       : 10s
=====
2018/10/17 13:33:59 Starting gobuster
=====
/admin.php (Status: 200)
/index.php (Status: 200)
/info.php (Status: 200)
/phpinfo.php (Status: 200)
/xmlrpc.php (Status: 200)
/xmlrpc_server.php (Status: 200)
=====
2018/10/17 13:35:16 Finished
=====
```

DNS Mode

Using **-m option** is enabled DNS mode which is effective for public network IP and extracts the sub-domains.

```
gobuster -m dns -u google.com -w /usr/share/wordlists/dirb/common.txt
```

As you can observe the output result from the given below result.

```
root@kali:~# gobuster -m dns -u google.com -w /usr/share/wordlists/dirb/common.txt

=====
Gobuster v2.0.0                OJ Reeves (@TheColonial)
=====
[+] Mode          : dns
[+] Url/Domain    : google.com
[+] Threads       : 10
[+] Wordlist      : /usr/share/wordlists/dirb/common.txt
=====
2018/10/17 13:27:32 Starting gobuster
=====
Found: accounts.google.com
Found: actions.google.com
Found: account.google.com
Found: admin.google.com
Found: Admin.google.com
Found: ADMIN.google.com
Found: ads.google.com
Found: alerts.google.com
Found: analytics.google.com
Found: answer.google.com
Found: ap.google.com
Found: apis.google.com
Found: api.google.com
Found: apps.google.com
Found: archive.google.com
Found: Archive.google.com
Found: asia.google.com
Found: Base.google.com
Found: base.google.com
Found: billing.google.com
Found: blogger.google.com
Found: Blog.google.com
Found: blog.google.com
Found: book.google.com
Found: bookmarks.google.com
Found: books.google.com
Found: Books.google.com
Found: Business.google.com
```

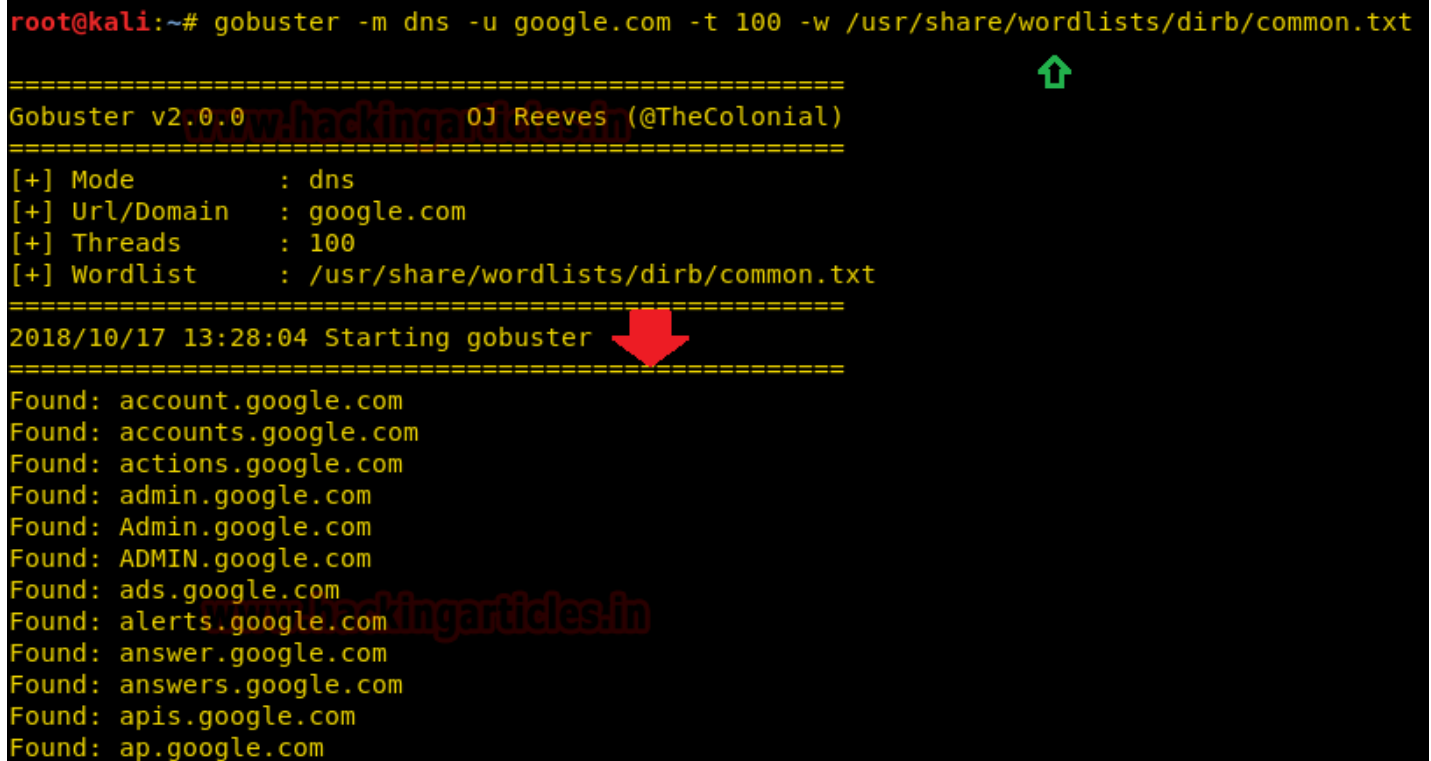
Set Threads Number

Using -t option, it enables the number of thread parameter to be applied while brute-forcing sub-domains name or directories.

```
gobuster -m dns -u google.com -t 100 -w /usr/share/wordlists/dirb/common.txt
```

```
root@kali:~# gobuster -m dns -u google.com -t 100 -w /usr/share/wordlists/dirb/common.txt

=====
Gobuster v2.0.0 OJ Reeves (@TheColonial)
=====
[+] Mode      : dns
[+] Url/Domain : google.com
[+] Threads   : 100
[+] Wordlist   : /usr/share/wordlists/dirb/common.txt
=====
2018/10/17 13:28:04 Starting gobuster
=====
Found: account.google.com
Found: accounts.google.com
Found: actions.google.com
Found: admin.google.com
Found: Admin.google.com
Found: ADMIN.google.com
Found: ads.google.com
Found: alerts.google.com
Found: answer.google.com
Found: answers.google.com
Found: apis.google.com
Found: ap.google.com
```



Obtain sub-domains IPs

Using **-i option** enables the IP parameter which should be showing IPs of extracted sub-domains.

```
gobuster -m dns -u google.com -t 100 -w /usr/share/wordlists/dirb/common.txt -i
```

From the given below result, you can observe that it showing IPv4 of Ipv6 for each extracted sub-domains.

```
root@kali:~# gobuster -m dns -u google.com -t 100 -w /usr/share/wordlists/dirb/common.txt -i
=====
Gobuster v2.0.0 OJ Reeves (@TheColonial)
=====
[+] Mode      : dns
[+] Url/Domain : google.com
[+] Threads   : 100
[+] Wordlist   : /usr/share/wordlists/dirb/common.txt
=====
2018/10/17 13:28:44 Starting gobuster
=====
Found: account.google.com [172.217.167.46, 2404:6800:4002:80b::200e]
Found: accounts.google.com [172.217.166.237, 2404:6800:4002:80b::200d]
Found: actions.google.com [172.217.167.46, 2404:6800:4002:80b::200e]
Found: Admin.google.com [172.217.167.46, 2404:6800:4002:80b::200e]
Found: ADMIN.google.com [172.217.167.46, 2404:6800:4002:80b::200e]
Found: admin.google.com [172.217.167.46, 2404:6800:4002:80b::200e]
Found: ads.google.com [172.217.167.46, 2404:6800:4002:80b::200e]
Found: alerts.google.com [172.217.167.46, 2404:6800:4002:80b::200e]
Found: answers.google.com [172.217.167.46, 2404:6800:4002:80b::200e]
Found: analytics.google.com [172.217.167.46, 2404:6800:4002:80b::200e]
Found: answer.google.com [172.217.167.46, 2404:6800:4002:80b::200e]
Found: ap.google.com [172.217.167.36, 2404:6800:4002:80b::2004]
Found: apis.google.com [172.217.167.46, 2404:6800:4002:80b::200e]
Found: apps.google.com [172.217.167.46, 2404:6800:4002:80b::200e]
Found: archive.google.com [172.217.167.46, 2404:6800:4002:80b::200e]
Found: Archive.google.com [172.217.167.46, 2404:6800:4002:80b::200e]
Found: asia.google.com [172.217.167.36, 2404:6800:4002:80b::2004]
Found: Base.google.com [172.217.167.46, 2404:6800:4002:80b::200e]
Found: base.google.com [172.217.167.46, 2404:6800:4002:80b::200e]
Found: api.google.com [172.217.167.36]
Found: billing.google.com [172.217.167.46, 2404:6800:4002:80b::200e]
Found: blog.google.com [172.217.167.41, 2404:6800:4002:80b::2009]
```

Force Processing Brute Force

It stops extracting the sub-domains name if meet any Wildcard DNS which is a non-existing domain, therefore uses **-fw option** to enable force processing parameter to continue the attack even if there is any Wildcard Domain.

```
gobuster -m dns -u google.com -t 100 -w /usr/share/wordlists/dirb/common.txt -fw
```

```

root@kali:~# gobuster -m dns -u google.com -t 100 -w /usr/share/wordlists/dirb/common.txt -fw
=====
Gobuster v2.0.0                                OJ Reeves (@TheColonial)
=====
[+] Mode      : dns
[+] Url/Domain : google.com
[+] Threads   : 100
[+] Wordlist   : /usr/share/wordlists/dirb/common.txt
=====
2018/10/17 13:29:23 Starting gobuster
=====
Found: account.google.com
Found: accounts.google.com
Found: actions.google.com
Found: ADMIN.google.com

```

Hide Process of Extracting

Using **-np option** hides the process of extracting sub-domains name while making brute force attack.

```
gobuster -m dns -u google.com -t 100 -w /usr/share/wordlists/dirb/common.txt -fw -np
```

```

root@kali:~# gobuster -m dns -u google.com -t 100 -w /usr/share/wordlists/dirb/common.txt -fw -np
=====
Gobuster v2.0.0                                OJ Reeves (@TheColonial)
=====
[+] Mode      : dns
[+] Url/Domain : google.com
[+] Threads   : 100
[+] Wordlist   : /usr/share/wordlists/dirb/common.txt
=====
2018/10/17 13:46:14 Starting gobuster
=====
Found: account.google.com
Found: actions.google.com
Found: accounts.google.com
Found: admin.google.com
Found: ADMIN.google.com
Found: Admin.google.com
Found: ads.google.com
Found: alerts.google.com
Found: analytics.google.com
Found: answers.google.com
Found: answer.google.com
Found: ap.google.com
Found: apis.google.com
Found: api.google.com
Found: apps.google.com
Found: base.google.com
Found: Base.google.com
Found: billing.google.com
Found: Blog.google.com
Found: book.google.com
Found: bookmarks.google.com
Found: Books.google.com
Found: books.google.com

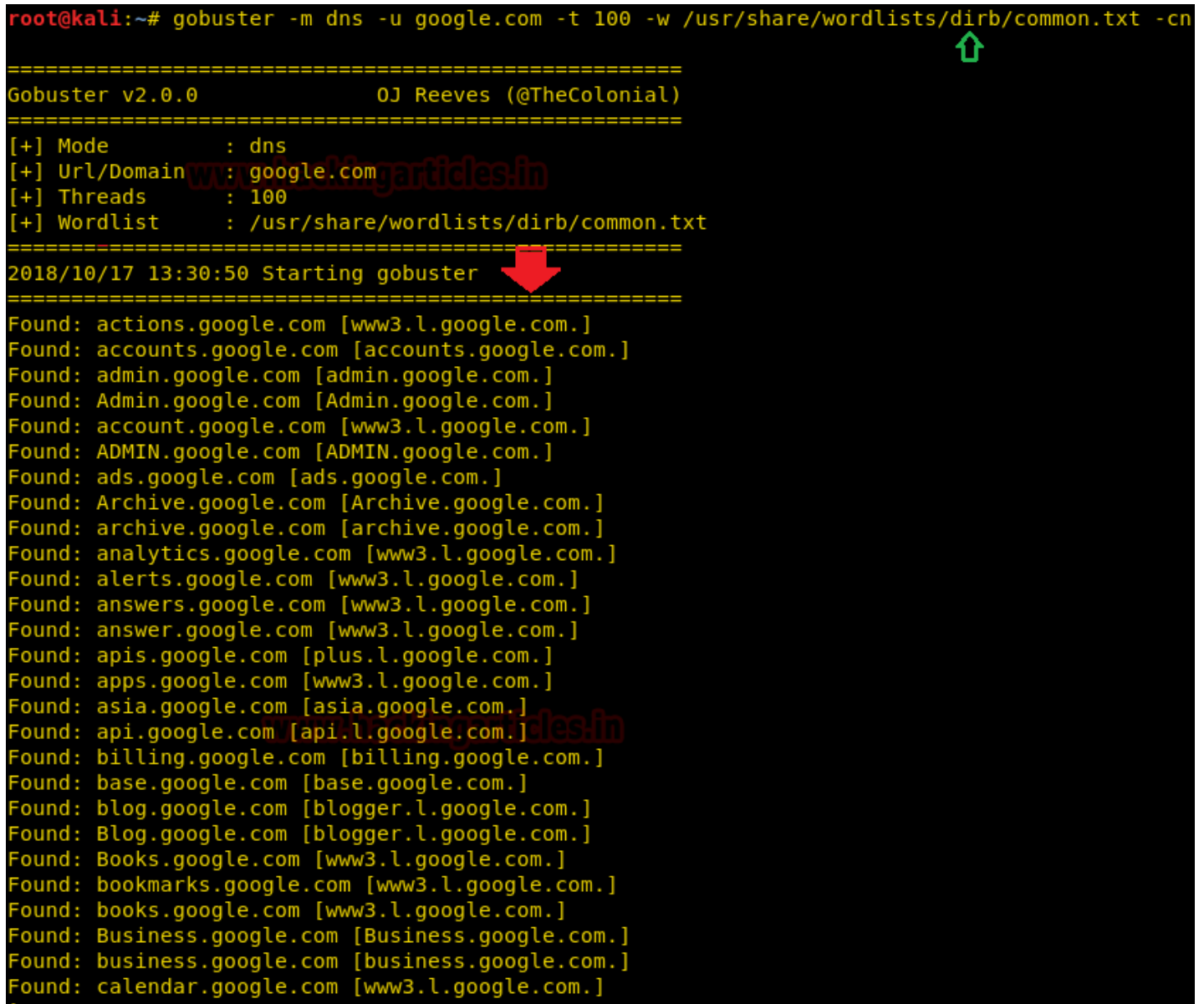
```

Extracting CNAME Records

Using **-cn option** enables CNAME Records parameter of the extracted sub-domains and show their CNAME records.

```
gobuster -m dns -u google.com -t 100 -w /usr/share/wordlists/dirb/common.txt -cn
```

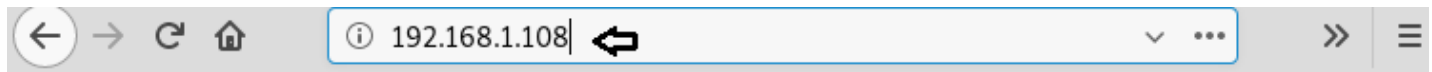
You can observe the output for above-executed command in the given below result.



```
root@kali:~# gobuster -m dns -u google.com -t 100 -w /usr/share/wordlists/dirb/common.txt -cn
=====
Gobuster v2.0.0                                OJ Reeves (@TheColonial)
=====
[+] Mode           : dns
[+] Url/Domain     : google.com
[+] Threads       : 100
[+] Wordlist       : /usr/share/wordlists/dirb/common.txt
=====
2018/10/17 13:30:50 Starting gobuster
=====
Found: actions.google.com [www3.l.google.com.]
Found: accounts.google.com [accounts.google.com.]
Found: admin.google.com [admin.google.com.]
Found: Admin.google.com [Admin.google.com.]
Found: account.google.com [www3.l.google.com.]
Found: ADMIN.google.com [ADMIN.google.com.]
Found: ads.google.com [ads.google.com.]
Found: Archive.google.com [Archive.google.com.]
Found: archive.google.com [archive.google.com.]
Found: analytics.google.com [www3.l.google.com.]
Found: alerts.google.com [www3.l.google.com.]
Found: answers.google.com [www3.l.google.com.]
Found: answer.google.com [www3.l.google.com.]
Found: apis.google.com [plus.l.google.com.]
Found: apps.google.com [www3.l.google.com.]
Found: asia.google.com [asia.google.com.]
Found: api.google.com [api.l.google.com.]
Found: billing.google.com [billing.google.com.]
Found: base.google.com [base.google.com.]
Found: blog.google.com [blogger.l.google.com.]
Found: Blog.google.com [blogger.l.google.com.]
Found: Books.google.com [www3.l.google.com.]
Found: bookmarks.google.com [www3.l.google.com.]
Found: books.google.com [www3.l.google.com.]
Found: Business.google.com [Business.google.com.]
Found: business.google.com [business.google.com.]
Found: calendar.google.com [www3.l.google.com.]
Found: ...
```

Proxy URL

Using **-p option** enables proxy URL to be used for all requests, by default it works on port 1080. As you can observe, on exploring target network IP in the web browser it put up “Access forbidden error” which means this web page is running behind some proxy.



Access forbidden!

You don't have permission to access the requested directory. There is either no index document or the directory is read-protected.

If you think this is a server error, please contact the [webmaster](#).

Error 403

[192.168.1.108](#)

Apache

To ensure this prediction, we run the gobuster command twice, firstly on port 80 which is by default and further on port 3129 along with **-p option** which enables proxy parameter.

```
gobuster -u http://192.168.1.108/ -w /usr/share/wordlists/dirb/common.txt
gobuster -u http://192.168.1.108/ -w /usr/share/wordlists/dirb/common.txt -p 1
```

From the given below image, you can take reference for the output result obtained for above commands, here we haven't obtained any directory or file on executing the first command where else in the second command executed successfully.

```

root@kali:~# gobuster -u http://192.168.1.108/ -w /usr/share/wordlists/dirb/common.txt ↩️
=====
Gobuster v2.0.0                OJ Reeves (@TheColonial)
=====
[+] Mode           : dir
[+] Url/Domain     : http://192.168.1.108/
[+] Threads       : 10
[+] Wordlist       : /usr/share/wordlists/dirb/common.txt
[+] Status codes   : 200,204,301,302,307,403
[+] Timeout       : 10s
=====
2018/10/23 13:09:24 Starting gobuster
=====
2018/10/23 13:09:24 [-] Wildcard response found: http://192.168.1.108/eb1d5338-62bf-43ef-b664-2289617915d5 => 403
2018/10/23 13:09:24 [!] To force processing of Wildcard responses, specify the '-fw' switch.
=====
2018/10/23 13:09:24 Finished
=====
root@kali:~# gobuster -u http://192.168.1.108/ -w /usr/share/wordlists/dirb/common.txt -p 192.168.1.108:3129 ↩️
2018/10/23 13:09:48 [!] proxy URL is invalid (parse 192.168.1.108:3129: first path segment in URL cannot contain colon)
root@kali:~# gobuster -u http://192.168.1.108/ -w /usr/share/wordlists/dirb/common.txt -p http://192.168.1.108:3129
=====
Gobuster v2.0.0                OJ Reeves (@TheColonial)
=====
[+] Mode           : dir
[+] Url/Domain     : http://192.168.1.108/
[+] Threads       : 10
[+] Wordlist       : /usr/share/wordlists/dirb/common.txt
[+] Status codes   : 200,204,301,302,307,403
[+] Proxy         : http://192.168.1.108:3129
[+] Timeout       : 10s
=====
2018/10/23 13:10:05 Starting gobuster
=====
/.htaccess (Status: 403)
/.htpasswd (Status: 403)
/.hta (Status: 403)
/blog (Status: 301)
/index.html (Status: 200)
=====
2018/10/23 13:10:12 Finished
=====
root@kali:~#

```

Author: Shubham Pandey is a Technical Writer, Researcher and Penetration tester contact [here](#)

◀ PREVIOUS POST

Magic Unicorn – PowerShell Downgrade Attack
and Exploitation tool

NEXT POST ▶

Meterpreter File System Commands Cheatsheet

4 thoughts on “Comprehensive Guide on Gobuster Tool”



Vdi

April 24, 2019 at 4:58 pm

Wow, this is very useful. Just what I was looking for. Thanks Raj.



Viorel Mocanu

April 29, 2021 at 3:36 pm

Hi, Raj! What other pentesting tools can you recommend beyond Gobuster?



Raj Chandel ✎

April 29, 2021 at 3:54 pm

ffuf



Viorel Mocanu

May 2, 2021 at 8:35 am

Thank you! What do you think about pentest-tools.com?

Comments are closed.

Join Our Training Program





Categories

Cryptography & Steganography

CTF Challenges

Cyber Forensics

Database Hacking

Footprinting

Hacking Tools

Kali Linux

Nmap

Others

Password Cracking

Penetration Testing

Pentest Lab Setup

Privilege Escalation

Red Teaming

Social Engineering Toolkit

Uncategorized

Website Hacking

Window Password Hacking

Wireless Hacking

Wireless Penetration Testing

Archives

Select Month



You may like

Best Alternative of Netcat Listener

64-bit Linux Assembly and Shellcoding

